

3hawn AO 106 (Rev. 06/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri

In the Matter of the Search of)
3 electronic devices (target devices #1 - #3) described in)
Attachment A, for evidence described in Attachment B) Case No. 4:21 MJ 1416 (JMB)
(List of information/items to be seized) currently being held)
as evidence located within the Eastern District of Missouri.) SUBMITTED TO THE COURT AND
SIGNED BY RELIABLE ELECTRONIC MEANS

APPLICATION FOR A SEARCH WARRANT

I, DAVID MORTON, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:
3 electronic devices (target devices #1 - #3) described in Attachment A, for evidence described in Attachment B (List of information/items to be seized) currently being held as evidence located within the Eastern District of Missouri,

located in the EASTERN District of MISSOURI, there is now concealed

SEE ATTACHMENT B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Title 21, U.S.C., §§ 846, 841(a)(1)

Offense Description

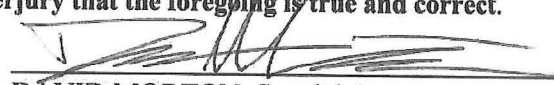
Conspiracy to possess with intent to distribute controlled substance(s)

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.


DAVID MORTON, Special Agent
Drug Enforcement Administration

Printed name and title

Sworn to, attested to, and affirmed before me via
reliable electronic means pursuant to Federal Rules of
Criminal Procedure 4.1 and 41.

Date: November 18, 2021

City and State: St. Louis, MO

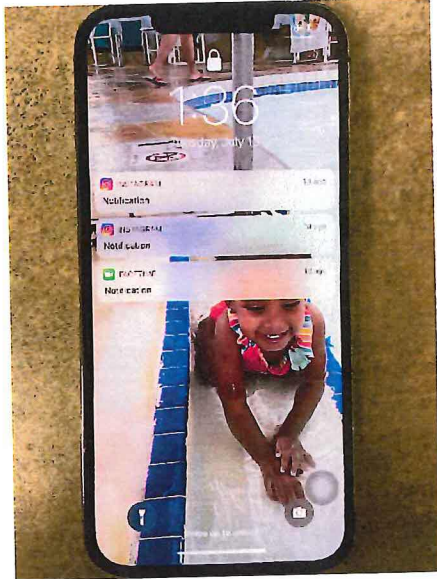

Judge's signature

John M. Bodenhause, U.S. Magistrate Judge

Printed name and title

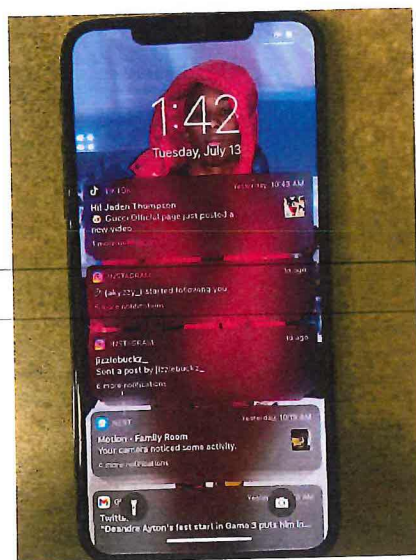
AUSA: STEPHEN CASEY

ATTACHMENT A



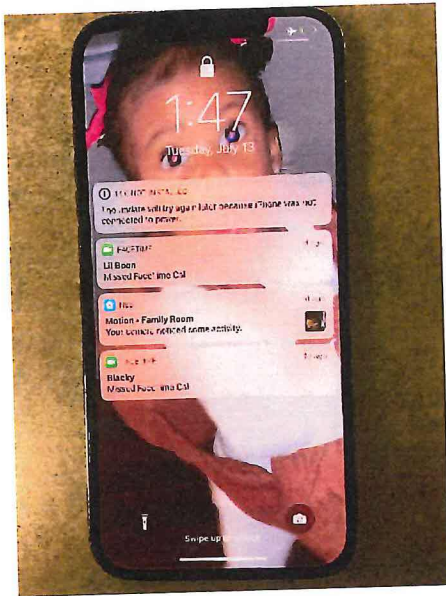
Device #1:

One grey in color iPhone containing one T-Mobile SIM card #8901260282769246539, phone number: unknown, found on A'Shontyn WATTS at the time of his arrest. Device #1 was seized by DEA as Exhibit N-50, and was sealed inside evidence bag #S001419028.



Device #2:

One grey in color iPhone containing one Verizon SIM card #89148000005919299677, phone number: unknown, found on A'Shontyn WATTS at the time of his arrest. Device #2 was seized by DEA as Exhibit N-51, and was sealed inside evidence bag #S001419029.



Device #3:

One blue in color iPhone containing one Sprint SIM card #89312530000229184439, phone number: unknown, found on A'Shontyn WATTS at the time of his arrest. Device #3 was seized by DEA as Exhibit N-52, and was sealed inside evidence bag #S001419030.

ATTACHMENT B

1. All fruits, instrumentalities, and records that relate to violations of Title 21, United States Code, Section 841(a) and 846 (unlawful manufacture, distribution, or possession with intent to distribute a controlled substance and conspiracy) involving A'Shontyn Watts and/or his identified and unidentified co-conspirators, including:
 - a. lists of customers and related identifying information;
 - b. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
 - c. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);
 - d. any information recording Watts or his unidentified co-conspirator's schedules or travel to include any GPS data saved or stored on the devices to be searched.
 - e. all bank records, checks, money orders, credit card bills, account information, and other financial records.
 - f. Images or video regarding the manufacture, distribution, or possession of controlled substances or any related financial transactions.
 - g. Any information related to the manufacturing, processing, or distributing of controlled substances or drug proceeds.
 - h. Graphic interchange formats and/or photographs, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI and MPEG) containing matter pertaining to the manufacture and distribution of controlled substances and controlled substance analogs and the laundering of proceeds of the same.

- i. Electronic mail, chat logs, Internet Relay Chat (IRC) log files and electronic messages, concerning the trafficking of controlled substances and controlled substance analogs through interstate or foreign commerce, including by United States mail or by computer, visual depictions, and records pertaining to the manufacture and distribution of controlled substances and controlled substance analogs and the laundering of proceeds of the same.
 - j. Log files and other records concerning dates and times of connection to the Internet and to websites pertaining to the manufacture and distribution of controlled substances and controlled substance analogs and the laundering of proceeds of the same.
 - k. Any Instant Message conversations, chats, e-mails, text messages, or letters pertaining to the manufacture and distribution of controlled substances and controlled substance analogs and the laundering of proceeds of the same.
 - l. Any social media to include Facebook, Snapchat, Instagram, LinkedIn, Twitter, or WhatsApp which contain conversations, chats, e-mails, text messages, or photographs that pertain to the manufacture and distribution of controlled substances and controlled substance analogs and the laundering of proceeds of the same.
2. Evidence of user attribution showing who used or owned the items to be searched at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;
- As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored,

including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

**AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH AND SEIZURE
WARRANT**

I, David Morton, being duly sworn, depose and state:

I. INTRODUCTION

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of the electronic devices described in Attachment A, currently in law enforcement possession, and the extraction from those devices of electronically stored information described in Attachment B.

2. I am a Special Agent with the Drug Enforcement Administration (DEA), and have been so employed since May 2018. I am currently assigned to the DEA's St. Louis Division Office (SLDO), specifically Group 33. I have completed the in-resident, 18 week DEA Basic Agent Training program at the DEA Academy in Quantico, Virginia, which provided extensive training in all aspects of the investigation of drug trafficking activities and organizations. Prior to my employment with the DEA, I was a Soldier in the United States Army for over six years and served as an enlisted Special Agent of the United States Army Criminal Investigation Command (CID) for the three years prior to my employment with DEA. As a CID Special Agent, I specialized in investigations related to fraud, sexual assault, and physical and sexual assaults upon children.

3. I am familiar with and have used normal methods of investigation, including, but not limited to, visual and electronic surveillance, questioning of defendants and witnesses, the use of search and arrest warrants, the use of pen registers, the use of undercover agents, the use of confidential sources, and the use of court-authorized wire intercepts. Based upon my training, experience, and understanding of this investigation, I believe that individuals engaged in drug

trafficking and money laundering often keep and maintain certain evidence of their crimes in their electronic devices, to include the items set forth in Attachment E.

4. The statements in this affidavit are based in part on my own participation in the investigation described below, as well as information provided by other law enforcement officials, and on my experience, training and background. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation.

II. DEVICES TO BE SEARCHED

5. This affidavit is submitted in support of an application for the issuance of a search warrant for the following items (hereafter collectively referred to as the "Devices"):

- a. Device #1: One grey colored iPhone containing one T-Mobile SIM card
#8901260282769246539, phone number: unknown, found on A'Shontyn WATTS at the time of his arrest. Device #1 was seized by DEA as Exhibit N-50, and was sealed inside evidence bag #S001419028.
- b. Device #2: One grey in color iPhone containing one Verizon SIM card
#89148000005919299677, phone number: unknown, found on A'Shontyn WATTS at the time of his arrest. Device #2 was seized by DEA as Exhibit N-51, and was sealed inside evidence bag #S001419029.
- c. Device #3: One blue in color iPhone containing one Sprint SIM card
#89312530000229184439, phone number: unknown, found on A'Shontyn WATTS at the time of his arrest. Device #3 was seized by DEA as Exhibit N-52, and was sealed inside evidence bag #S001419030.

6. The Devices are currently in the possession of the DEA. As described in greater detail below, the Devices were all seized from A'Shontyn WATTS on July 12, 2021 during the arrest of WATTS by members of the St. Louis County Police Department, Intelligence Unit.

7. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

III. TECHNICAL TERMS

8. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device. A wireless telephone may have wireless connection capabilities such as Wi-Fi and Bluetooth.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special

sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication Devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the internet, connections between devices on the internet often cross state and international borders, even when the devices communicating with each other are in the same state.

9. Based on my training, experience, and research, I know that the Devices have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation Device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the Devices.

IV. OVERVIEW OF INVESTIGATION

10. I am part of an experienced team of drug investigators that is investigating the drug trafficking activities of A'Shontyn WATTS. This investigation has established evidence that WATTS and others are engaged in a conspiracy to distribute controlled substances in violation of Title 21, United States Code, Sections 841(a)(1) and 846; and laundering of monetary instruments in violation of Title 18, United States Code, Sections 1956 and 1957. WATTS is part of the Troy EDWARDS drug trafficking organization (DTO) operating primarily in the St. Louis, Missouri metropolitan area.

11. As described in further detail below, evidence obtained sources including from telephone toll records, Title III wiretaps, confidential source information, and geolocation information indicates WATTS is engaged in drug trafficking activities. WATTS has been identified as a trusted associate of EDWARDS.

12. On July 12, 2021, members of the St. Louis County Police Department, Intelligence Unit, arrested WATTS for his involvement with a north St. Louis County, Missouri nightclub shooting, which resulted in the seizure of the Devices from WATTS' person.

V. PROBABLE CAUSE

Initial Investigation of WATTS

13. On August 7, 2018, St. Louis DEA Group 33 investigators approached WATTS at the St. Louis Lambert International Airport, St. Louis, Missouri, as he waited to board an early morning flight to Los Angeles. WATTS provided vague and changing information about his purpose for travel to Los Angeles, which investigators know is a source city for controlled substances. WATTS consented to investigators' request to search his carry-on bag and checked bags. Investigators located and seized \$34,896.00 in United States currency (USC) from WATTS. Following the discovery of the currency, a police drug detection canine positively alerted to the presence of illegal narcotics on the USC.¹ At the time of the seizure, WATTS provided investigators with telephone number (314) 276-1311.

14. Following this seizure, investigators conducted a criminal record search of WATTS and discovered a March 5, 2018 arrest citation for Violation of the Missouri Controlled Substance Law. On the arrest citation, WATTS provided a St. Louis Metropolitan Police Department officer with telephone number (314) 265-8268. I reviewed WATTS' publicly accessible social media accounts and learned that WATTS was close friends with EDWARDS.

WATTS' Historical Usage of Phones to Facilitate Drug Trafficking

1. WATTS later contested the seizure. The seized currency was returned to WATTS so as to avoid triggering discovery proceedings that would reveal the ongoing investigation of WATTS, EDWARDS, and others that resulted from this initial seizure from WATTS as detailed later in this affidavit.

15. In February 2019, a DEA Confidential Source (hereinafter referred to as “the CS”), made a recorded call to WATTS at 314-265-8268, and negotiated the purchase of four (4) ounces of fentanyl for \$1,500.00 per ounce.

16. In March 2019, DEA St. Louis initiated court-authorized interception of the voice and text message conversations of phone number (314) 265-8268 used by WATTS. In May 2019, DEA St. Louis resumed interception of WATTS using phone number (314) 265-8268 and initiated interception of phone number (314) 399-1748, which was also determined to be in use by WATTS. The communications intercepted on these telephones indicated WATTS was engaged in the nearly daily distribution of marijuana, and also learned that WATTS did not appear to be employed by a business or other conventional employer.

Telephonic Communications Pertaining to a Money Seizure

17. On September 12, 2019 at approximately 9:49 p.m., during court-authorized interception of a phone used by EDWARDS, DEA St. Louis intercepted an outgoing call placed by EDWARDS to the unidentified male user of phone number 618-795-2239. During the call, EDWARDS stated “I been hit . . . I need her to get uh . . . Little A out of trouble. That nigga got my money and everything.” The unidentified male asked “[w]ho, Little A?” and EDWARDS responded “[y]eah man, they flagged him.” Investigators suspected that “Little A” referred to WATTS and know that “flagged” is a colloquial term that refers to being pulled over by the police.

18. Investigators later determined that on the evening of September 12, 2019, at approximately 9:41 p.m., WATTS, Dalarrion SCALES, and Jeremy HENLEY attempted to flee from East St. Louis, Illinois police officers in WATTS’ 2018 Jeep Track Hawk Sport Utility Vehicle (SUV) after ESLPD attempted to stop the vehicle. WATTS was the driver. The SUV ran

out of gas during the pursuit, and WATTS, SCALES and HENLEY fled the scene. WATTS and his associates were apprehended and found to be in possession of a large amount of marijuana, \$45,699.99 United States currency (believed to be EDWARDS' money), and a handgun.

Phone Tolls

19. Throughout the course of this investigation, agents have identified multiple phone numbers suspected of or confirmed to be in use by WATTS. I know from my training and experience that drug traffickers frequently use multiple telephones to facilitate their drug trafficking activities.

20. Throughout the multi-year investigation involving WATTS, I have noted that WATTS has consistently maintained use of phone numbers (314) 265-8268 and (314) 399-1748. In the experience of the investigative team, drug traffickers commonly possess multiple telephone numbers and periodically discontinue the use of some phone numbers and replace them with new numbers. This is done in an effort to frustrate law enforcement efforts to monitor the usage of a given device involved in drug trafficking activities. Conversely, WATTS has employed the same "dirty" phone numbers for several years. It is notable that the subscriber information for both aforementioned devices has not changed over the course of several years, indicating the same user has maintained the phones. Additionally, the Devices are all late-model iPhones, which contain significant storage capability. Based on these facts, I believe the Devices are capable of, and likely to possess, a volume of incriminating evidence that exceeds the storage and usage capabilities of the cheaper, smaller, "burner" phones frequently employed by suspected drug traffickers. Investigators obtained the tolls records of WATTS' (314) 314-1748 between June 4, 2021 and August 8, 2021. It is notable that the last outgoing communication

made by WATTS' (314) 314-1748 phone number during this timeframe was made on July 12, 2021, the same day he was arrested by St. Louis County Police Department officers.

21. A review of the phone tolls of WATTS' (314) 399-1748 phone number revealed repeated contact with phone numbers linked to drug trafficking.² Phone numbers in contact with WATTS' (314) 399-1748 phone number include:

a. **(314) 705-4566:** 22 outgoing calls between June 5, 2021 and June 24, 2021. This phone number was also listed in the iMessage and FaceTime call invitation logs of Kenneth THOMAS, a significant multi-kilogram polydrug distributor recently arrested in Tijuana, Mexico. A storage unit used by THOMAS was found to contain 12 kilograms of fentanyl. In December 2020, investigators received court authorization to conduct a search of an iCloud account that was determined to be in use by THOMAS. The FaceTime call invitation logs contained 16 FaceTime call invitations to WATTS' (314) 265-8268 phone number and one call invitation to WATTS' (314) 399-1748 phone number.³ THOMAS' iCloud account also contained a contact titled "Ashontyn," which listed phone number (314) 399-1748. THOMAS is currently charged with drug trafficking in Case Number 4:21CR554 SRC DDN.

b. **(314) 319-8181:** 19 outgoing calls between July 9, 2021 and July 11, 2021. The phone number is subscribed to Jon Kambell, P.O. Box 15955, Lenexa, KS 66285. Review of a DEA database linked the phone number to four separate, active DEA investigations; however,

2. It should be noted that the phone tolls of phone number (314) 265-8268 show the phone has continued to be used after WATTS was released from prison following his arrest on July 12, 2021. Consequently, investigators believe WATTS is still in possession of that telephone.

3. The FaceTime call invitation logs provided by Apple stated: "*These logs do not indicate that any communication between users actually took place. These logs indicate that the source handle initiated a FaceTime call to the recipient handle which was routed to Apple's servers. Apple has no information as to whether the FaceTime call was successfully established or information regarding duration of a FaceTime call. FaceTime call invitation logs where the calling device and the receiving device are both running iOS 10 or higher will not include instances of Invitation Accept and Invitation Reject."

the name Jon Kambell appears fictitious. The name Kambell appeared to be fictitious following multiple open source and law enforcement database queries. The use of a fictitious subscriber name for a particular phone number is a common method of tradecraft deployed by drug traffickers and money launderers as a way to avoid law enforcement detection and conceal the user's true identity.

c. **(314) 261-6126**: 14 outgoing calls between June 2, 2021 and July 11, 2021. The phone is subscribed to Casey Sanders, 3 Fernridge Drive, St. Peters, MO 63376. Review of a DEA database linked the phone number to approximately six separate, active DEA and FBI investigations. A law enforcement database query was conducted and resulted in a Casey Sanders having a criminal history of Possession of a Controlled Substance and Possession of Marijuana/Synthetic Cannabinoid in June 2019.

Drug Activity Involving WATTS

22. On March 11, 2021, DEA St. Louis and United States Postal Inspection Service (USPIS) investigators established surveillance of a suspicious vehicle parked in a hotel parking lot in Arnold, Missouri. At approximately 9:37 p.m., investigators observed a black-colored BMW sedan bearing an Illinois license plate drive into the hotel parking lot, then almost immediately drive out of the lot and begin to circle the parking lots of nearby businesses. Investigators believed the vehicle was conducting counter-surveillance in an attempt to identify the presence of law enforcement.

23. Minutes later, investigators observed the BMW leave the vicinity of the hotel, then travel back in to the area and park several parking spaces away from the suspicious vehicle. Investigators then observed a man later identified as Kendrez MURPHY exit the BMW, immediately walk to the front driver's side wheel, and then reach briefly into the wheel well

before walking to the trunk of the car. MURPHY then opened the vehicle's trunk and leaned into the trunk to retrieve multiple brick-shaped items from a bag in the trunk.

24. Investigators, wearing vests with "Police" placards clearly visible on their chests and yelling "police," detained MURPHY after he attempted to flee on foot. MURPHY was found in possession of two phones, one of which he stated was currently being used to FaceTime. By the time investigators retrieved the phones from the ground, no active FaceTime call was observed.

25. Group Supervisor (GS) Tiras Cunningham and I interviewed MURPHY. After being advised of his rights per Miranda, MURPHY stated he was sent to the hotel by WATTS. MURPHY stated he regularly picks up loads of marijuana on behalf of WATTS and is paid \$500.00 and a pound of marijuana each time he retrieves the marijuana for WATTS. MURPHY stated at other times, he will purchase between 30 and 40 pounds of marijuana from WATTS to sell.

26. MURPHY stated he was in the downtown St. Louis, MO area earlier that night when he was contacted by WATTS. MURPHY related that WATTS asked him to travel to the hotel to retrieve something from a vehicle and provided him with the hotel address. MURPHY stated he did not know what he was retrieving until he observed the brick-shaped objects in the duffel bag. MURPHY related when WATTS contacted him to ask that MURPHY go to the hotel, WATTS spontaneously told MURPHY that he (WATTS) would never put MURPHY in a bad situation and stated he (WATTS) would pay MURPHY \$2,000.00 to retrieve the bag from the vehicle in the hotel parking lot. MURPHY stated he was FaceTiming with WATTS as he walked to the vehicle and was told by WATTS to retrieve the vehicle's key from the front driver side wheel well. MURPHY stated he believed WATTS was simultaneously FaceTiming a second

individual as he was in contact with MURPHY. MURPHY stated he knew that whatever he was supposed to retrieve from the vehicle was supplied by “Pimpin” who he described as WATTS’ uncle. Investigators know that “Pimpin” is the nickname of THOMAS. MURPHY was then released from the scene.

Seizure of the Devices

27. On July 12, 2021, investigators with the St. Louis County Police Department, Intelligence Unit arrested WATTS for his involvement in a north St. Louis County, Missouri night club shooting. At the time of his arrest, WATTS was in possession of Device #1, Device #2, and Device #3. It should be mentioned, the night club where the shooting occurred is owned by Davante Lindsey, who is an associate of members of the EDWARDS DTO, and is suspected of operating his own independent DTO.

28. On July 13, 2021, SA Christopher Most and I obtained the Devices from Detective Matthew King with the St. Louis County Police Department, Bureau of Crimes Against Persons, and then transported the Devices to the DEA St. Louis Division Office where the Devices were submitted to the Non-Drug Evidence Vault for safekeeping pending an application of a search warrant to forensically search them. Throughout the time in law enforcement custody, based on my training and experience, I know that the Devices have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the device first came into the possession of the investigative agency(ies).

VI. EVIDENCE LIKELY TO BE FOUND IN THE DEVICES

29. Based on phone toll analysis, I believe WATTS possesses multiple telephones and telephone numbers at once, and does not changes phone numbers or discontinue service to previously used phone numbers, as other typical drug traffickers do.

30. I also know that wireless telephones possess applications that can be used to store drug transaction information, ledgers, contact information, and other such records. This data can also be synchronized across devices and stored on other wireless telephones, tablets, and/or computers if the user makes use of a cloud-based storage service or manually transfers records from device to device.

31. Wireless telephones are also frequently used to communicate via various messaging applications. I am aware that drug traffickers frequently use end-to-end encrypted communication applications to securely communicate with their co-conspirators. These applications are sometimes designed to purge those communications after their transmission from any external server associated with the application, thus making the data impossible to retrieve remotely. I also know that a wireless telephone's storage options can be adjusted to prevent uploading of data to a cloud-based storage platform. As a consequence of traffickers' use of secure messaging applications and localized storage, I know that wireless devices can sometimes be the sole storage media where certain communications, images, and financial transaction records are stored and retrievable. Investigators believe the phones likely used by WATTS to communicate with co-conspirators contain valuable evidence of their drug trafficking conspiracy, coordination, and other illegal potential illegal activities, such as information pertaining to the north St. Louis County, Missouri night club shooting.

32. Wireless telephones can also possess text messages, call logs, and other records of communications that serve as valuable evidence in a drug conspiracy. From my training and experience, I know that drug traffickers sometimes use encrypted communications applications, such as iMessage and Signal, which allow traffickers to communicate securely without a means for law enforcement to capture the content of those communications. These messages may be stored solely on the device used to send such messages, making it the only container of such evidence. Based on intercepted calls and text messages, investigators know that WATTS makes also makes use of “FaceTime” video calling to communicate with EDWARDS and other associates, and specifically to discuss drug trafficking activities. FaceTime call logs can serve as valuable evidence of attempted or actual communication between individuals, and FaceTime call logs are only stored by Apple for a short period of time. Consequently, such call logs contained on the Devices themselves may constitute evidence that cannot be obtained through any other means than a forensic examination of the Devices.

33. I also know that drug dealers can use wireless phones to access social media accounts. Many social media platforms contain direct messaging capabilities, which enable individuals to privately communicate with other users of the application. The investigative team know from their training and experience that drug traffickers sometimes use such private messaging applications to facilitate their drug trafficking activities, and that these messages can be stored on, and accessible from, a seized device.

34. I know that drug traffickers often take pictures using their phones showing them holding large sums of United State currency, as a way to “flash” or show off their wealth. These pictures usually also include expensive jewelry, clothing, firearms, drugs, vehicles, homes, and

other assets. Sometimes these pictures are taken with other associates. Investigators know that these pictures are often taken with, and stored within, cellular telephones such as the Devices.

VII. ELECTRONIC STORAGE AND FORENSIC ANALYSIS

35. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

36. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

37. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Devices to human inspection in order to determine whether it is evidence described by the warrant.

VIII. CONCLUSION

38. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

39. Because this warrant seeks only permission to examine the Devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion

onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

40. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, *i.e.*, post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

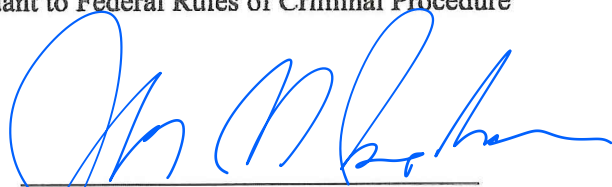
I state under the penalty of perjury that the foregoing is true and correct.

11/18/2021
DATE



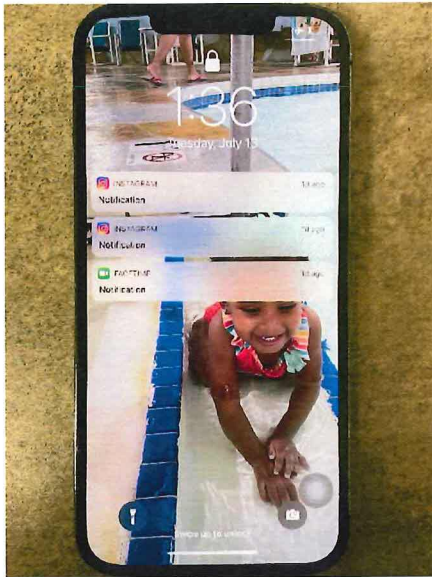
DAVID MORTON
Special Agent
Drug Enforcement Administration

Sworn to, attested to and affirmed before me pursuant to Federal Rules of Criminal Procedure 4.1 and 41 this 18th day of November, 2021.



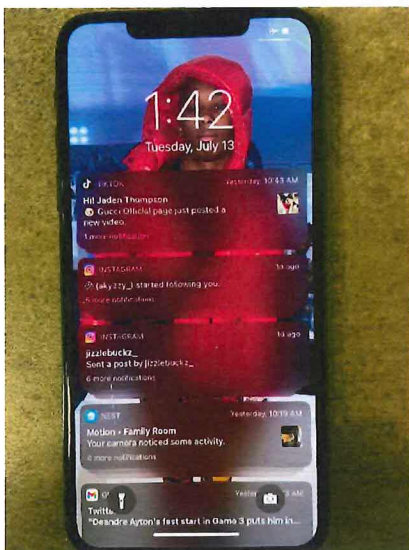
JOHN M. BODENHAUSEN
UNITED STATES MAGISTRATE JUDGE
Eastern District of Missouri

ATTACHMENT A



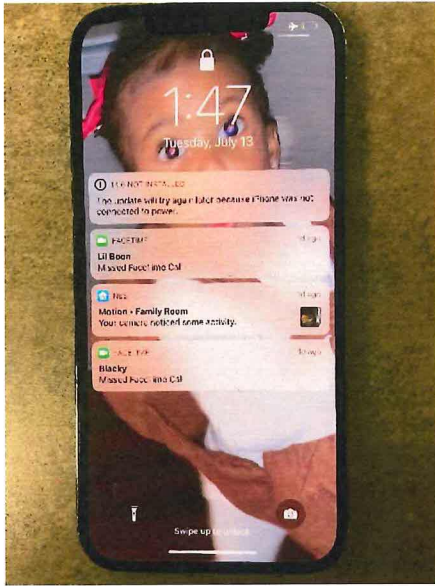
Device #1:

One grey in color iPhone containing one T-Mobile SIM card #8901260282769246539, phone number: unknown, found on A'Shontyn WATTS at the time of his arrest. Device #1 was seized by DEA as Exhibit N-50, and was sealed inside evidence bag #S001419028.



Device #2:

One grey in color iPhone containing one Verizon SIM card #89148000005919299677, phone number: unknown, found on A'Shontyn WATTS at the time of his arrest. Device #2 was seized by DEA as Exhibit N-51, and was sealed inside evidence bag #S001419029.



Device #3:

One blue in color iPhone containing one Sprint SIM card #89312530000229184439, phone number: unknown, found on A'Shontyn WATTS at the time of his arrest. Device #3 was seized by DEA as Exhibit N-52, and was sealed inside evidence bag #S001419030.

ATTACHMENT B

1. All fruits, instrumentalities, and records that relate to violations of Title 21, United States Code, Section 841(a) and 846 (unlawful manufacture, distribution, or possession with intent to distribute a controlled substance and conspiracy) involving A'Shontyn Watts and/or his identified and unidentified co-conspirators, including:
 - a. lists of customers and related identifying information;
 - b. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
 - c. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);
 - d. any information recording Watts or his unidentified co-conspirator's schedules or travel to include any GPS data saved or stored on the devices to be searched.
 - e. all bank records, checks, money orders, credit card bills, account information, and other financial records.
 - f. Images or video regarding the manufacture, distribution, or possession of controlled substances or any related financial transactions.
 - g. Any information related to the manufacturing, processing, or distributing of controlled substances or drug proceeds.
 - h. Graphic interchange formats and/or photographs, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI and MPEG) containing matter pertaining to the manufacture and distribution of controlled substances and controlled substance analogs and the laundering of proceeds of the same.

- i. Electronic mail, chat logs, Internet Relay Chat (IRC) log files and electronic messages, concerning the trafficking of controlled substances and controlled substance analogs through interstate or foreign commerce, including by United States mail or by computer, visual depictions, and records pertaining to the manufacture and distribution of controlled substances and controlled substance analogs and the laundering of proceeds of the same.
 - j. Log files and other records concerning dates and times of connection to the Internet and to websites pertaining to the manufacture and distribution of controlled substances and controlled substance analogs and the laundering of proceeds of the same.
 - k. Any Instant Message conversations, chats, e-mails, text messages, or letters pertaining to the manufacture and distribution of controlled substances and controlled substance analogs and the laundering of proceeds of the same.
 - l. Any social media to include Facebook, Snapchat, Instagram, LinkedIn, Twitter, or WhatsApp which contain conversations, chats, e-mails, text messages, or photographs that pertain to the manufacture and distribution of controlled substances and controlled substance analogs and the laundering of proceeds of the same.
2. Evidence of user attribution showing who used or owned the items to be searched at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored,

including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.